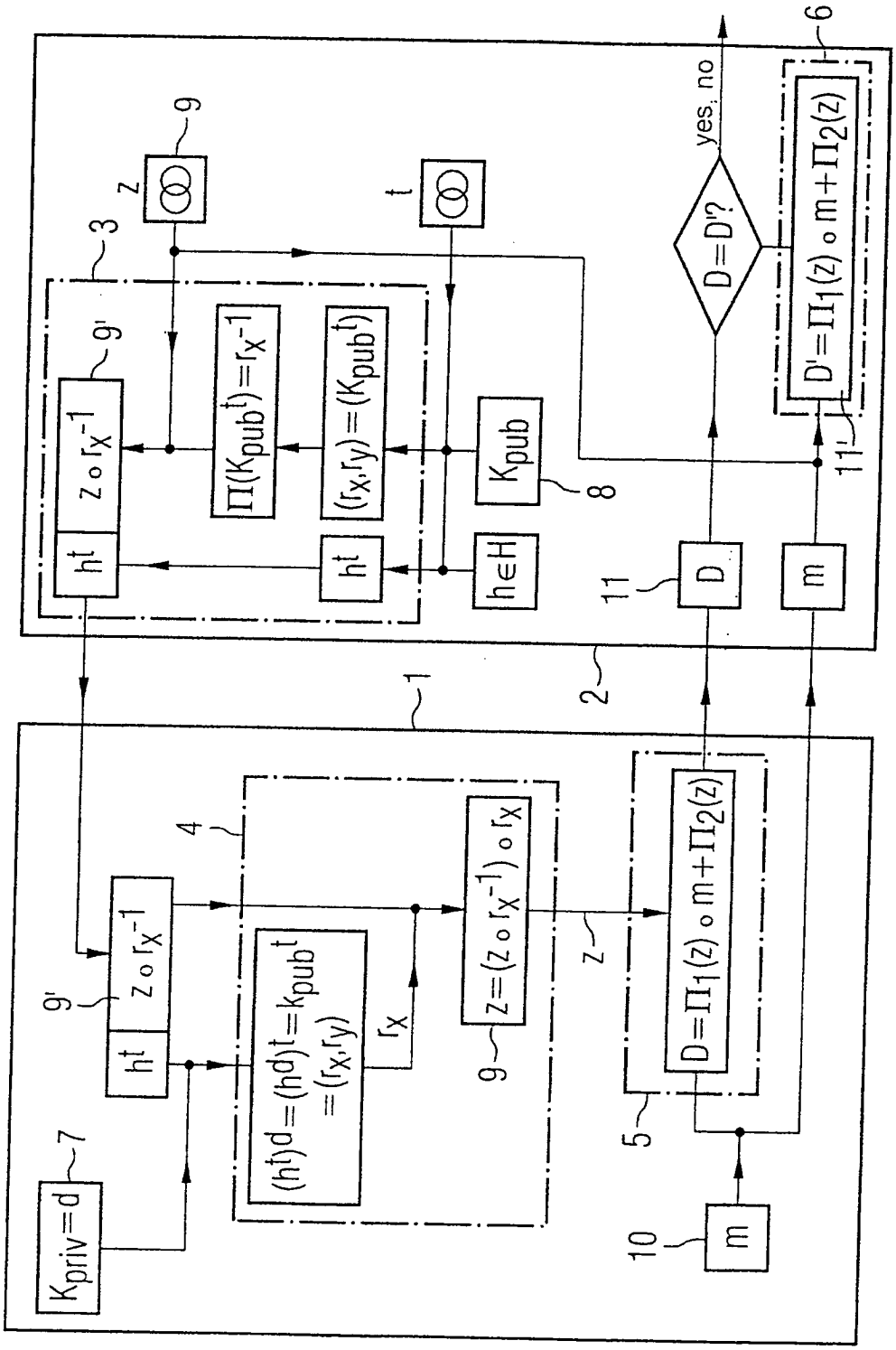
1
2
3
4
5
6
7
8
9
10
11
11'
9'
z
t
yes, no
D=D'?
D'=Π1(z) ∘ m+Π2(z)
D=Π1(z) ∘ m+Π2(z)
Kpriv=d
Kpub
h∈H
D
m
z ∘ rX-1
ht
Π(Kpubt)=rX-1
(rX,rY)=(Kpubt)
(ht)d=(hd)t=kpubt =(rX,rY)
rX
z=(z ∘ rX-1) ∘ rX